Docket No. 42390P10855
Express Mail No.: EM014067254US

UNITED STATES PATENT APPLICATION
FOR

METHOD AND SYSTEM FOR PROVIDING BUS ENCRYPTION BASED ON CRYPTOGRAPHIC KEY EXCHANGE

Inventors:

Michael S. Ripley
Brendan S. Traw

Prepared by:

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP
12400 Wilshire Boulevard, Seventh Floor
Los Angeles, California 90025-1026
(310) 207-3800

METHOD AND SYSTEM FOR PROVIDING BUS ENCRYPTION BASED ON CRYPTOGRAPHIC KEY EXCHANGE

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention generally relates to encrypting and decrypting data transmitted over a data bus, and in particular, to a method and system for protecting digital content stored on a storage medium from unauthorized copying.

Description of the Related Art

[0002] A variety of techniques are available for protecting digital contents stored on a storage medium from unauthorized copying such as scrambling and encryption/decryption techniques. However, the integrity of some copy protection techniques has been compromised and such copy protection techniques are no longer effective against unauthorized copying of copyrighted material. For example, in the field of digital versatile disc (DVD) technology, the integrity of content scramble system (CSS) for scrambling DVD video contents has been recently compromised by hackers, and software programs are now available that can descramble the contents of CSS-protected DVDs, using a computer equipped with a DVD-ROM drive.

[0003] Additionally, digital contents on a storage medium is usually transmitted from a storage device (i.e., any device capable of accessing data from a storage medium) to a host device (i.e., any device capable of retrieving data from the storage device) over a data bus in a form that can be captured by anyone having the proper equipment. Although the data transmitted may not be in its original digital form (i.e., data may be encrypted and/or scrambled), a copy of the encrypted and/or scrambled data captured at the time of the transmission may still be playable by presenting the encrypted data to a host device as though it was coming from a legitimate storage device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] Figure 1 is a block diagram of a system for protecting digital content stored on a storage medium from copying according to one embodiment of the present invention.

[0005] Figure 2 is a block diagram of a system for protecting DVDs from malicious copying according to one embodiment of the invention.

[0006] Figure 3 is a flowchart of encrypting data prior to transmitting the data over a bus according to one embodiment of the invention.

[0007] Figure 4 is a flowchart of decrypting data transmitted over a bus according to one embodiment of the invention.

[0008] Figure 5 is a flowchart of decrypting and descrambling DVD contents according to one embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0009] In the following description, specific details are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to one skilled in the art that the present invention may be practiced without these specific details. In other instances, well-known circuits, structures and techniques have not been shown in detail in order to avoid obscuring the present invention.

[00010] Figure 1 depicts a system 100 for protecting digital content stored on a storage medium from copying according to one embodiment of the present invention. The copy protection system 100 includes a storage device 102 coupled to a host device 104 via a data bus 106 to enable transmission of data (e.g., encrypted and/or non-encrypted data) between the storage and host devices through the bus. The storage device 102 may be any device capable of accessing data from a storage medium 108. The host device 104 may be any device capable of retrieving data from the storage device 102. The storage device 102 may be a stand-alone device arranged in an enclosure separate from the host device 104 or alternatively, the storage device 102 and the host device 104 may be combined into one enclosure. The storage medium 108 placed within the storage device 102 may be any type of a removable or non-removable storage medium suitable for storing digital content including, but not limited to, digital versatile discs (DVDs), CD-ROMs, optical discs, magneto-optical discs, flash-based memory, floppy disks, hard drives, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, magnetic or optical cards.

[00011] To implement the copy protection system 100, media

manufacturers will place a key distribution data block (e.g., media key block "MKB" 110) generated by an authorized entity (i.e., an entity responsible for establishing and administering the copy protection system) on each piece of storage media. In one embodiment, the MKB 110 is a block of encrypted keys that can be embedded in a storage medium such that storage devices that access the content from the storage medium are able to process portion(s) of the MKB to compute a secret key that can be used to encrypt the data prior to transmitting the data over the bus. The host device that plays the content from the storage medium also accesses and processes portion(s) of the MKB to compute the same secret key to properly decrypt the data transmitted over the bus.

[00012] As seen by referring to figure 1, the storage device 102 includes an encryption subsystem 114 according to one embodiment of the invention to encrypt the content read from the storage medium 108 prior to transmitting the data over the bus 106 to the host device 104 to prevent unauthorized copying. Included in the encryption system 114 is a set of device keys 116, a MKB processing logic 118, a one-way function 122 and an encryption logic 126. The set of device keys 116 has been assigned to each storage device when manufactured. These device keys are provided by the authorized entity and are used by the MKB processing logic 118 to process portion(s) of the MKB 110 embedded in the storage medium 108 to compute a secret media key 120. The device keys 116 may either be unique to each individual storage device, or used commonly by multiple storage devices. In one embodiment, the MKB, the device keys and the MKB processing logic are configured such that the same secret media key will be generated regardless of which compliant device is used to access the storage medium so long as its device keys have not been compromised.

[00013] The host device 104 connected to the storage device 102 includes a decryption subsystem 128 according to one embodiment of the invention to decrypt the data supplied from the storage device. Included in the decryption subsystem 128 are its own set of device keys 130 and a MKB processing logic 132 to process the MKB 110 using its own set of device keys to compute a secret media key 134. Although the set of device keys 130 assigned to the host device 104 may be different from the device keys 116 assigned to the storage device

102, the media key 134 generated by the host device 104 will be the same as the media key 120 generated by the storage device 102 provided that neither sets of device keys have been compromised.

[00014] Also included in the copy protection system 100 is a random number generator 136 to generate a random or sequential number (referred hereinafter as "nonce") and send a copy of it to the storage device 102. The storage device 102 combines the nonce 144 received from the host device 104 with the media key 120 using the one-way function 122 and returns the result (i.e., bus key 124) to the encryption logic 126. The one-way function 122 is configured such that the bus key 124 can be generated by inputting the media key 120 and the nonce 144, however, determining the media key 120 from the bus key 124 and nonce 144 is computationally infeasible. When the nonce 144 is supplied from the host device 104 to the storage device 102, the nonce 146 is also accessed by the one-way function 138 residing within the host device 104 to combine the media key 134 and the nonce 146 to produce its own bus key 140 to be used by the decryption logic 142. It should be noted that since the same one-way function is used by the storage device 102 and host device 104, both storage and host devices will generate the same bus key provided that same media key and nonce was used by both devices to generate the bus key.

[00015] In one embodiment, some sort of a tamper resistant scheme is employed to tightly couple the logical components within the encryption subsystem 114 and the decryption subsystem 128 so that secret keys and data flowing between the logical components are not accessible from outside. In this regard, the data flowing within the encryption and decryption subsystems are protected by a tamper resistant scheme; however, the data bus 106 connecting the storage device 102 to the host device 104 may be unsecured and may be susceptible to access by an attacker. To protect the data transmitted over the data bus 106 which may be non-secured against malicious copying, the digital content 112 read from the storage medium 108 is encrypted by the encryption logic 126 with the bus key 124 prior to transmitting over the data bus 106 to the host device 104. In this regard, only the host device 104 with the correct bus key can properly decrypt the encrypted data 148 transmitted over the bus 106.

[00016] Advantageously, the copy protection system 100 of the present

invention is effective in resisting against "Replay" attack. In replay attack, an attacker reroutes the encrypted data 148 going from the storage device 102 to the host device 104 and records the encrypted data onto a recordable medium. Additionally, when the host device 104 accesses the MKB 110 embedded in the storage medium 108, the attacker also records the MKB 110 onto the same recordable medium. The copy of the MKB 110 and encrypted data 148 captured at the time of transmission may be played on a conventional media player system by presenting the encrypted data to the host device as though it was coming from a legitimate storage device. However, in the present invention, since the nonce value used by the host device to generate its decryption bus key during replay of the enciphered data will be different than the nonce value used by the storage device to generate its encryption bus key at the time of enciphering, this type of replay attack will be prevented. In other words, by using the nonce to generate the bus keys, the bus key 140 obtained by the host device 104 during subsequent access of the enciphered data will most likely be different than the bus key 124 that was previously used to encrypt the enciphered data and therefore the host device will not be able to properly decrypt the enciphered data.

[00017] In one implementation, if a set of device keys is compromised in a way that threatens the integrity of the copy protection system, new media can be released containing an updated MKB that causes the compromised set of device keys to calculate an incorrect media key, thereby revoking its ability to work with the new media. This means that devices with the compromised set of device keys will no longer function with new media while other existing compliant devices with valid device keys will continue to work with new media.

[00018] It should be noted that there are a variety of ways to derive a secret key from public key distribution system and that the usage of media key block (MKB) is just one example of distributing cryptographic keys and the details of public key management may vary among different applications. In this regard, other types of public key distribution system can be utilized with the copy protection system of the present invention. Such is within the scope and contemplation of the present invention.

[00019] Referring to Figure 3, the operations of encrypting data prior to

transmitting the data over a bus according to one embodiment of the invention are shown. When a compliant storage medium is placed within the storage device, the MKB processing logic responsible for computing a media key accesses the MKB from the storage medium (block 300). Then, the MKB processing logic generates a media key using a set of device keys assigned to the storage device and the MKB read from the storage medium (block 310). In one implementation, the MKB comprises a block of encrypted data, where each encrypted data is a secret media key encrypted with a different key. Each device key may be data of a predefined bit size (e.g., 56 bit data) that includes an index number used to indicate which encrypted data within the MKB data block the device key is configured to decrypt. By decrypting the designated portion of the MKB using the device key, a secret media key may be obtained. This means that the secret media key contained in the MKB can be obtained by any device that has a legitimate set of device keys. After the compliant storage medium has been placed in the storage device and prior to any encryption taking place, the host device generates a nonce (e.g., a random number) and sends the nonce to the storage device. The encryption subsystem receives the nonce sent by the host device (block 320) and combines it with the media key obtained above using a one-way function to produce a bus key (block 330). Using the bus key obtained, the encryption subsystem encrypts the digital content read from the storage medium and outputs the encrypted data to the host device through the bus (block 340).

[00020] Referring to Figure 4, the operations of decrypting data transmitted over a bus according to one embodiment of the invention are shown. When the host device needs to access the storage medium in the storage device, the MKB processing logic residing within the decryption subsystem of the host device reads the MKB from the storage medium (block 400). Then in block 410, the MKB processing logic generates a media key using a set of device keys assigned to the host device and the MKB read from the storage medium. As noted earlier, the decryption subsystem generates a nonce (block 420) and sends a copy of it to the encryption subsystem (block 430) and sends another copy of it to the one-way function of the decryption subsystem. Then, the decryption subsystem combines the nonce and the media key by using the one-way function to produce a bus key (block 440). The bus key is

used by the decryption subsystem to decrypt the encrypted data transmitted over the bus (block 450).

[00021] Figure 2 depicts a system 200 for protecting digital versatile discs (DVDs) from unauthorized copying according to one embodiment of the invention. In this embodiment, the copy protection system 200 uses the media key block (MKB) 210 as described above to patch scrambled contents 212 of DVD 208 to provide additional copy protection. In this regard, the format of new compliant DVDs may remain unchanged (i.e., content scramble system (CSS) scrambling is still used), except that a MKB 210 is introduced as a new data element on the disc. As noted earlier, the MKB 210 is a block of encrypted data that allows different devices using different individually-assigned device keys to extract a common secret key, called the media key. The usage of MKB 210 to patch scrambled DVD data 212 enables a protection system to be renewed (i.e., if a set of device keys is compromised in the future, a new MKB can be used that excludes just that set of compromised device keys from the system).

[00022] As part of the copy protection system 200 of the invention, new compliant DVD drives 202 are equipped with device keys 218, MKB processing logic 220, one-way function 224 and encryption logic 228 necessary to process the MKB and extract its secret media key 222, to calculate a bus key 226 based on the media key 222 and a nonce 250, and encrypt the data 212 on the DVD 208, which is CSS scrambled, using the bus key 226. The DVD video player software 230 of the host computer 204 (e.g., host PC or DVD player) is also equipped with these additional features to access and process MKB 210 using its own set of device keys 232 to compute a secret media key 236, to calculate a bus key 242 based on the media key 236 and the nonce 252, and decrypt the data 254 transmitted by the DVD drive 202 using the bus key 242.

[00023] When a new compliant DVD-Video disc 208 is inserted into the DVD drive 202, the following key exchange procedure occurs between the DVD drive 202 and host PC 204. The DVD drive 202 reads the MKB 210 and uses its device keys 218 to calculate the media key 222. The DVD video player software 230 running on the host PC 204 sends the necessary command to the DVD drive 202 to allow it to also read the MKB 210 and use its device keys 232 to calculate the media key 236. The DVD video player software 230 selects a

number (nonce) at random 238, and sends that number to the DVD drive 202 using a predefined command. The DVD drive 202 and DVD video player software 230 both calculate a common bus key 226, 242, which is derived from a cryptographic one-way function of the media key and nonce. Subsequently, the DVD video player software 230 sends requests to the DVD drive 202 to read the descramble keys 214 (e.g., CSS keys) and CSS-scrambled content 212 from the disc 208. Before sending the CSS keys 214 or CSS-scrambled content 212 to the host PC 204, the DVD drive 202 first encrypts them using a robust cipher and the bus key 226. Upon receipt of the data, the DVD video player software 230 decrypts them using the same cipher and bus key 242 and forwards the data to the descramble logic 246. The descramble logic 246 uses the descramble keys 214 to descramble the data and forwards the data to a decompression logic 248.

[00024] For the calculation of the media key and bus key, and for the bus encryption and decryption of the CSS keys and CSS-scrambled content, a robust cipher with a large key size is used. In one implementation, the cipher is the C2 cipher, and the key size is 56 bits.

[00025] In this embodiment, the copy protection system of the present invention dramatically improves the protection for DVD-Video content by "wrapping" a robust protection scheme around the old CSS scheme. This is accomplished in a simple and novel way, using MKB technology to provide for renewal in the event that device keys are compromised in the future, and adding a nonce to protect against replay attacks.

[00026] Referring to Figure 5, the operations of decrypting and descrambling DVD contents according to one embodiment of the invention are shown. When a DVD is inserted in the DVD-ROM drive, the DVD video player software running in the host PC may request descramble keys or secret data (e.g., CSS keys) required for descrambling the scrambled content from the DVD drive (block 500). Then in block 510, the DVD drive encrypts the CSS keys read from the disc with bus key and sends them to the host PC. The CSS keys are encrypted prior to sending them over the bus to the host PC. The CSS keys are encrypted using the bus key that can also be computed by the host PC having a set of non-compromised device keys as previously discussed. In this regard, once the encrypted CSS keys have been received, the DVD video player

software running in the host PC decrypts the CSS keys with the bus key (block 520). Then in block 530, the DVD video player software dispatches requests to read the CSS-scrambled content to the DVD drive. Before sending the content to the host PC, the DVD drive encrypts the scrambled content using the bus key and sends the encrypted data to the host PC (block 540). Upon receipt of the content, the DVD video player software first decrypts the data using the bus key (block 550). The output of the decryption logic is supplied to the descramble logic which performs the CSS descramble process using the DSS keys obtained earlier (block 560).

[00027] While the foregoing embodiments of the invention have been described and shown, it is understood that variations and modifications, such as those suggested and others within the spirit and scope of the invention, may occur to those skilled in the art to which the invention pertains. The scope of the present invention accordingly is to be defined as set forth in the appended claims.